

EQUIVARIANT GAUSS SUM OF FINITE QUADRATIC FORMS

SHOUHEI MA

ABSTRACT. The classical quadratic Gauss sum can be thought of as an exponential sum attached to a quadratic form on a cyclic group. We introduce an equivariant version of Gauss sum for arbitrary finite quadratic forms, which is an exponential sum twisted by the action of the orthogonal group. We prove that simple arithmetic formulae hold for some basic classes of quadratic forms. In application, such invariant appears in the dimension formula for certain vector-valued modular forms.

1. INTRODUCTION

In his study of the quadratic reciprocity law, Gauss introduced and evaluated the exponential sum $\sum_{x=0}^{p-1} e(ax^2/p)$ where $a \in \mathbb{F}_p^\times$, which is now called the Gauss sum. Here $e(z) = \exp(2\pi iz)$ for $z \in \mathbb{Q}/\mathbb{Z}$. If we consider the \mathbb{Q}/\mathbb{Z} -valued quadratic form $q(x) = 2^{-1}ax^2/p$ on the cyclic group $A = \mathbb{Z}/p$ and the associated bilinear form $(x, y) = q(x+y) - q(x) - q(y)$, the Gauss sum can be written in the form $G(A) = \sum_{x \in A} e((x, x))$. Gauss evaluated such an exponential sum also for $A = \mathbb{Z}/p^k$ (see [1]). If we consider $G(A)$ for general finite quadratic forms A , we have essentially no further problem concerning evaluation because the product formula $G(A_1 \oplus A_2) = G(A_1) \cdot G(A_2)$ holds and A can be decomposed into cyclic forms as above and certain special forms on $\mathbb{Z}/2^k \oplus \mathbb{Z}/2^k$ (see [6]).

In this paper we introduce an equivariant version of $G(A)$ for a finite quadratic form $A = (A, q)$, which is a twist of $G(A)$ by the orthogonal group $O(A) = O(A, q)$. Let $(,) : A \times A \rightarrow \mathbb{Q}/\mathbb{Z}$ be the associated bilinear form as above. In general, for a subgroup Γ of $O(A)$, we define

$$G(A, \Gamma) = \sum_{[x] \in \Gamma \backslash A} \sum_{y \in \Gamma x} e((x, y)).$$

The classical Gauss sum $G(A)$ is the case $\Gamma = \{\text{id}\}$. We are interested in the case $\Gamma = O(A)$, the motivation coming from certain modular forms (§6). If $A = \oplus_p A_p$ is the decomposition into p -parts, we have (Corollary 2.2)

$$G(A, O(A)) = \prod_p G(A_p, O(A_p)).$$

Supported by Grant-in-Aid for Scientific Research (S) 15H05738.

Hence we may restrict our attention to quadratic forms on p -groups.

Our main result is an arithmetic formula of $G(A, O(A))$ for some basic quadratic forms, which has similar but different shape from that of $G(A)$. For simplicity we state the result only for $p > 2$, referring to §4 for the case $p = 2$. We write $(\frac{\cdot}{p})$ for the Legendre symbol.

Theorem 1.1 (§3). *Let $p > 2$.*

(1) *Let A be the symmetric bilinear form $(x, y) = axy/p^k$ on \mathbb{Z}/p^k where $a \in \mathbb{Z}_p^\times$. Then*

$$G(A, O(A)) = \begin{cases} 0, & p^k \equiv 3 \pmod{4}, \\ \left(\frac{a}{p}\right)^k \sqrt{|A|}, & p^k \equiv 1 \pmod{4}. \end{cases}$$

(2) *Let A be a p -elementary form (quadratic space over \mathbb{F}_p) of dimension $m > 1$. When A contains an isotropic vector, then*

$$G(A, O(A)) = \begin{cases} 0, & p \equiv 3 \pmod{4}, \\ 2 \left(\frac{2\delta}{p}\right)^m \left(\frac{d(A)}{p}\right) \sqrt{|A|}, & p \equiv 1 \pmod{4}. \end{cases}$$

Here $d(A) \in \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$ is the discriminant of A , and $\delta \in \mathbb{F}_p$ is a square root of -1 which exists when $p \equiv 1 \pmod{4}$. When A is the anisotropic plane, we have $G(A, O(A)) = (-1)^{(p+1)/2} p$.

(3) *Let $A = A_1 \oplus A_2$ where $A_1 \simeq \mathbb{Z}/p^k$ is a cyclic form as in (1) with $k > 1$ and A_2 is a p -elementary form as in (2). Then*

$$G(A, O(A)) = G(A_1, O(A_1)) \cdot G(A_2, O(A_2)).$$

The product formula in (3) is not trivial because $O(A)$ does not preserve the decomposition $A = A_1 \oplus A_2$ in general. When $p = 2$, $k \leq 3$, this formula does not hold. The formula in (2) already shows that the most naive product formula does not hold.

We were led to considering such an orbital exponential sum through the study of certain vector-valued modular forms. The Gauss sum $G(A, O(A))$ appears in the dimension formula for them. We explain this in §6. In that formula also arises the following variant of $G(A, O(A))$:

$$G'(A, O(A)) = \sum_{[x] \in O(A) \setminus A} e(-q(x)) \sum_{y \in O(A)_x} e((x, y)).$$

We show that a similar arithmetic formula holds for $G'(A, O(A))$. We state the result only for $p > 3$, referring to §5 for the case $p = 2, 3$.

Theorem 1.2 (§5). *Let $p > 3$.*

(1) *If A is a cyclic form as in Theorem 1.1 (1), then*

$$G'(A, O(A)) = \frac{1}{2} \left(1 + \left(\frac{p}{3}\right)^k \right) \left(\frac{2a}{p}\right)^k \sqrt{|A|} \times \begin{cases} 1, & p^k \equiv 1 \pmod{4}, \\ \sqrt{-1}, & p^k \equiv 3 \pmod{4}. \end{cases}$$

(2) Let A be a p -elementary form as in Theorem 1.1 (2). When A contains an isotropic vector, we have

$$G'(A, O(A)) = \begin{cases} 0, & p \equiv 2 \pmod{3}, \\ 2\zeta_{16}^{m^2(p-1)^2} \left(\frac{2\delta}{p}\right)^m \left(\frac{(-1)^k d(A)}{p}\right) \sqrt{|A|}, & p \equiv 1 \pmod{3}. \end{cases}$$

Here $\zeta_{16} = e(1/16)$, $k = [m/2]$ and $\delta \in \mathbb{F}_p$ is a primitive 6-th root of 1 which exists when $p \equiv 1 \pmod{3}$. When A is the anisotropic plane, we have $G'(A, O(A)) = -\left(\frac{p}{3}\right)p$.

(3) If $A = A_1 \oplus A_2$ is a quadratic form as in Theorem 1.1 (3), we have

$$G'(A, O(A)) = G'(A_1, O(A_1)) \cdot G'(A_2, O(A_2)).$$

One finds that there are many cases of vanishing for both $G(A, O(A))$ and $G'(A, O(A))$. One also finds that the absolute values of $G(A, O(A))$ and $G'(A, O(A))$ are either 0 or $\sqrt{|A|}$ or $2\sqrt{|A|}$ in all cases we calculate.

Our evaluation of $G(A, O(A))$ and $G'(A, O(A))$ is done by direct calculation based on the explicit description of the $O(A)$ -orbits. This seems to be difficult for more general quadratic forms. The author does not know if there is more systematic way to evaluate $G(A, O(A))$ and $G'(A, O(A))$, and whether a uniform arithmetic formula holds for general finite quadratic forms.

2. BASIC DEFINITIONS

A *finite quadratic form* is a finite abelian group A equipped with a \mathbb{Q}/\mathbb{Z} -valued quadratic form $q : A \rightarrow \mathbb{Q}/\mathbb{Z}$. This means that $q(ax) = a^2q(x)$ for $a \in \mathbb{Z}$ and $x \in A$, and that the \mathbb{Q}/\mathbb{Z} -valued pairing

$$(x, y) = q(x + y) - q(x) - q(y), \quad x, y \in A,$$

is symmetric bilinear. Unless stated otherwise, we assume that (A, q) is nondegenerate, namely the bilinear form $(,)$ is nondegenerate. We often abbreviate $A = (A, q)$. The orthogonal direct sum of two finite quadratic forms A_1, A_2 is written as $A_1 \oplus A_2$. A map $A \rightarrow A$ is called isometry if it is an isomorphism of abelian groups and preserves q . The group of isometries of (A, q) is denoted by $O(A) = O(A, q)$ and called the orthogonal group of (A, q) . Finite quadratic forms are also called *finite quadratic modules* in some literatures. A standard example is the discriminant form L^\vee/L of an even lattice L , where the quadratic form q is defined by $q(x + L) = (x, x)/2 + \mathbb{Z}$ for $x \in L^\vee$. The associated bilinear form is the mod \mathbb{Z} reduction of the pairing on the dual lattice L^\vee .

Let A_p be the p -component of A . The canonical decomposition $A = \bigoplus_p A_p$ as an abelian group is automatically an orthogonal decomposition. Indecomposable quadratic forms on p -groups are classified by Wall [6]. When $p > 2$, quadratic forms on p -groups can be reconstructed from the

associated bilinear form by $q(x) = 2^{-1}(x, x)$, as 2 is invertible in \mathbb{Z}_p . We mainly consider the bilinear form $(\ , \)$ in this case. The 2-adic case is more subtle.

Let Γ be a subgroup of $O(A)$. We define the equivariant Gauss sum of (A, Γ) as the exponential sum

$$G(A, \Gamma) = \sum_{[x] \in \Gamma \backslash A} \sum_{y \in \Gamma x} e((x, y)).$$

This is well-defined: if we use γx in place of x where $\gamma \in \Gamma$, then

$$\sum_{y \in \Gamma x} e((\gamma x, y)) = \sum_{y \in \Gamma x} e((x, \gamma^{-1}y)) = \sum_{y \in \Gamma x} e((x, y)).$$

Similarly, we define the equivariant Gauss sum of the second kind by

$$G'(A, \Gamma) = \sum_{[x] \in \Gamma \backslash A} e(-q(x)) \sum_{y \in \Gamma x} e((x, y)).$$

When Γ is trivial,

$$G(A, \{\text{id}\}) = \sum_{x \in A} e((x, x)), \quad G'(A, \{\text{id}\}) = \sum_{x \in A} e(q(x)),$$

are the classical quadratic Gauss sum. We will write $G(A) = G(A, \{\text{id}\})$ and $G'(A) = G'(A, \{\text{id}\})$. The evaluation of $G(A)$ and $G'(A)$ is well-known: see [1]. We especially have the Milgram formula $G'(A) = e(\sigma(A)/8) \sqrt{|A|}$, where $\sigma(A) \in \mathbb{Z}/8\mathbb{Z}$ is the signature of A .

Our object of study is the case $\Gamma = O(A)$. In the rest of this paper, for two $O(A)$ -orbits $[x], [y] \in O(A) \backslash A$ we will write

$$\langle [x], [y] \rangle_A = \sum_{y' \in O(A)y} e((x, y')).$$

(We often omit A in the subscript.) This sum does not depend on the choice of an element x from $[x]$, as checked above. In particular, since $-\text{id} \in O(A)$, we see that $\langle [x], [y] \rangle$ is a real number. Note that $\langle [x], [y] \rangle \neq \langle [y], [x] \rangle$ in general. The equivariant Gauss sums can be written as

$$\begin{aligned} G(A, O(A)) &= \sum_{[x] \in O(A) \backslash A} \langle [x], [x] \rangle_A, \\ G'(A, O(A)) &= \sum_{[x] \in O(A) \backslash A} e(-q(x)) \langle [x], [x] \rangle_A. \end{aligned}$$

Then $G(A, O(A))$ is a real algebraic integer.

We first localize the equivariant Gauss sum to each prime.

Lemma 2.1. *Let A be of the form $A = A_1 \oplus A_2$ and assume that $\Gamma \subset O(A)$ can be decomposed as $\Gamma = \Gamma_1 \times \Gamma_2$ such that $\Gamma_i \subset O(A_i)$. Then*

$$G(A, \Gamma) = G(A_1, \Gamma_1) \cdot G(A_2, \Gamma_2), \quad G'(A, \Gamma) = G'(A_1, \Gamma_1) \cdot G'(A_2, \Gamma_2).$$

Proof. For $x = (x_1, x_2) \in A_1 \oplus A_2$ the orbit Γx is decomposed as $\Gamma x = (\Gamma_1 x_1) \times (\Gamma_2 x_2)$. Hence

$$\begin{aligned} G(A, \Gamma) &= \sum_{[(x_1, x_2)] \in \Gamma \backslash A} \sum_{(y_1, y_2) \in \Gamma x} e((x_1, y_1) + (x_2, y_2)) \\ &= \sum_{[x_1] \in \Gamma_1 \backslash A_1} \sum_{[x_2] \in \Gamma_2 \backslash A_2} \sum_{y_1 \in \Gamma_1 x_1} \sum_{y_2 \in \Gamma_2 x_2} e((x_1, y_1)) \cdot e((x_2, y_2)) \\ &= G(A_1, \Gamma_1) \cdot G(A_2, \Gamma_2). \end{aligned}$$

The case of $G'(A, \Gamma)$ is similar. \square

For $\Gamma = O(A)$ we have the canonical decomposition $O(A) = \prod_p O(A_p)$. Hence we obtain

Corollary 2.2. *We have*

$$G(A, O(A)) = \prod_p G(A_p, O(A_p)), \quad G'(A, O(A)) = \prod_p G'(A_p, O(A_p)).$$

The evaluation of $G(A, O(A))$ and $G'(A, O(A))$ is thus reduced to the case of quadratic forms on p -groups. For $G(A, O(A))$ we study the case $p > 2$ in §3 and the case $p = 2$ in §4. We study $G'(A, O(A))$ in §5.

3. NONDYADIC CASE

Let $p > 2$. Let A be an abelian p -group endowed with a \mathbb{Q}/\mathbb{Z} -valued symmetric bilinear form (\cdot, \cdot) . In this section we evaluate $G(A, O(A))$ for the following quadratic forms: (1) cyclic forms, (2) p -elementary forms (quadratic spaces over \mathbb{F}_p), and (3) direct sum $A = A_1 \oplus A_2$ where A_i is as in (i). We write $A(\varepsilon)$ for the scaling of A by $\varepsilon \in \mathbb{Z}_p^\times$. The symmetric bilinear form on \mathbb{Z}/p^k defined by $(x, y) = axy/p^k$, $a \in \mathbb{Z}_p^\times$, is denoted by $A_{p^k, a}$. We write $\left(\frac{\cdot}{p}\right)$ for the Legendre symbol. We also write $\zeta_{p^k} = e(1/p^k)$.

3.1. Cyclic forms.

Proposition 3.1. *Let $A = A_{p^k, a}$ with $p > 2$. Then*

$$G(A, O(A)) = \begin{cases} 0, & p \equiv 3 \pmod{4}, k \text{ odd}, \\ \left(\frac{a}{p}\right)^k \sqrt{p^k}, & \text{otherwise.} \end{cases}$$

Proof. The orthogonal group $O(A)$ consists of $\pm \text{id}$, and $-\text{id}$ fixes no nonzero element. Hence

$$G(A, O(A)) = 1 + \frac{1}{2} \sum_{\substack{x \in \mathbb{Z}/p^k \\ x \neq 0}} (\zeta_{p^k}^{ax^2} + \zeta_{p^k}^{-ax^2}) = \text{Re}(G(A)).$$

By [1] Theorem 1.5.2 we have

$$G(A) = \left(\frac{a}{p^k}\right) \sqrt{p^k} \times \begin{cases} 1, & p^k \equiv 1 \pmod{4}, \\ \sqrt{-1}, & p^k \equiv 3 \pmod{4}. \end{cases}$$

So $\text{Re}(G(A)) = 0$ when $p^k \equiv 3 \pmod{4}$, and $\text{Re}(G(A)) = \left(\frac{a}{p}\right)^k \sqrt{p^k}$ otherwise. \square

3.2. p -elementary forms. Let A be a symmetric form on a p -elementary group with $p > 2$. We can naturally view A as a quadratic space over \mathbb{F}_p . By Witt's extension theorem ([4] Theorem 2.44), two nonzero vectors of A are $O(A)$ -equivalent if and only if they have the same norm. For $\mu \in \mathbb{F}_p$ let A_μ be the subset of A of vectors x such that $(x, x) = \mu$. Then

$$A = \{0\} \cup (A_0 \setminus \{0\}) \cup \bigcup_{\mu \in \mathbb{F}_p^\times} A_\mu$$

is the $O(A)$ -orbit decomposition of A .

We first consider the case A has a nonzero isotropic vector. In that case A contains as a direct summand the *hyperbolic plane* U , namely the symmetric form on $\mathbb{F}_p \oplus \mathbb{F}_p$ given by the Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. As the first step we calculate the case $A = U$.

Lemma 3.2. *We have $G(U, O(U)) = (1 + (-1)^{(p-1)/2})p$.*

Proof. Let u_1, u_2 be the standard basis of U . Then $U_0 = \mathbb{F}_p u_1 \cup \mathbb{F}_p u_2$, and for $\mu \neq 0$ we have $U_\mu = \{v u_1 + v^{-1}(2^{-1}\mu)u_2 \mid v \in \mathbb{F}_p^\times\}$. As a reference vector in U_μ for $\mu \in \mathbb{F}_p$ we take

$$x_\mu = u_1 + (2^{-1}\mu)u_2 \in U_\mu.$$

We write for $\mu, \lambda \in \mathbb{F}_p$

$$(3.1) \quad \langle \mu, \lambda \rangle_U = \sum_{x \in U_\lambda} \zeta_p^{(x_\mu, x)} = \sum_{v \in \mathbb{F}_p^\times} \zeta_p^{2^{-1}(\mu v + \lambda v^{-1})}.$$

We have

$$\langle \mu, \lambda \rangle_U = \begin{cases} \langle U_\mu \setminus \{0\}, U_\lambda \rangle, & \lambda \neq 0, \\ \langle U_\mu \setminus \{0\}, U_0 \setminus \{0\} \rangle + 1, & \lambda = 0. \end{cases}$$

The second equality of (3.1) holds even when $\lambda = 0$ (both sides equal to -1 when $\mu \neq 0$, and to $p - 1$ when $\mu = 0$). This expression shows that $\langle \mu, \lambda \rangle_U = \langle \lambda, \mu \rangle_U$.

By definition we have

$$(3.2) \quad G(U, O(U)) = \sum_{\mu \in \mathbb{F}_p} \langle \mu, \mu \rangle_U = \sum_{v \in \mathbb{F}_p^\times} \sum_{\mu \in \mathbb{F}_p} \zeta_p^{2^{-1}\mu(v + v^{-1})}.$$

When $p \equiv 1 \pmod{4}$, the equation $v + v^{-1} = 0$ has two solutions, namely the square roots of -1 , hence $G(U, O(U)) = 2p$. When $p \equiv 3 \pmod{4}$, we have $v + v^{-1} \neq 0$ for any $v \in \mathbb{F}_p^\times$. Thus $G(U, O(U)) = 0$ in this case. \square

We consider the general case.

Proposition 3.3. *Let A be an m -dimensional quadratic space over \mathbb{F}_p with $p > 2$ that contains a nonzero isotropic vector. Let $d(A) \in \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$ be the discriminant of A . When $p \equiv 1 \pmod{4}$, we choose $\delta \in \mathbb{F}_p$ with $\delta^2 = -1$. Then*

$$G(A, O(A)) = \begin{cases} 0, & p \equiv 3 \pmod{4}, \\ 2 \left(\frac{2\delta}{p} \right)^m \left(\frac{d(A)}{p} \right) \sqrt{|A|}, & p \equiv 1 \pmod{4}. \end{cases}$$

Proof. We keep the notation in the proof of Lemma 3.2. We choose a splitting $A = U \oplus B$, which gives the partition

$$A_\mu = \bigsqcup_{\lambda \in \mathbb{F}_p} U_\lambda \times B_{\mu-\lambda}.$$

As a reference vector in A_μ we use $(x_\mu, 0) \in U_\mu \times B_0$. Then

$$(3.3) \quad G(A, O(A)) = \sum_{\mu, \lambda \in \mathbb{F}_p} |B_{\mu-\lambda}| \cdot \langle \mu, \lambda \rangle_U$$

by this partition. The formula of $|B_\alpha|$ can be found in [4] §2.8. It depends on the parity of $m = \dim(A)$.

(1) Let $m = 2k$ be even. We write $\delta_A = \left(\frac{(-1)^k d(A)}{p} \right)$. Then $\delta_A = 1$ if and only if $B \simeq U^{k-1}$. By [4] Theorem 2.59 we have

$$|B_\alpha| = \begin{cases} p^{k-2}(p^{k-1} + \delta_A p - \delta_A) & \alpha = 0, \\ p^{k-2}(p^{k-1} - \delta_A) & \alpha \neq 0. \end{cases}$$

In particular, $|B_\alpha|$ for $\alpha \neq 0$ is independent of α and hence

$$(3.4) \quad G(A, O(A)) = |B_0| \cdot G(U, O(U)) + |B_1| \cdot \sum_{\substack{\mu, \lambda \in \mathbb{F}_p \\ \mu \neq \lambda}} \langle \mu, \lambda \rangle_U.$$

Since

$$(3.5) \quad \sum_{\mu, \lambda \in \mathbb{F}_p} \langle \mu, \lambda \rangle_U = \sum_{\mu \in \mathbb{F}_p} \sum_{x \in U} \zeta_p^{(x_\mu, x)} = 0,$$

we have

$$G(A, O(A)) = (|B_0| - |B_1|) \cdot G(U, O(U)) = p^{k-1} \cdot \delta_A \cdot G(U, O(U)),$$

and the proposition follows from Lemma 3.2.

(2) Let $m = 2k + 1$ be odd. We put $\tilde{d}(A) = (-1)^k d(A)$. Then $B \simeq U^{k-1} \oplus \langle \tilde{d}(A) \rangle$. By [4] Theorem 2.60 we have for $\alpha \in \mathbb{F}_p$

$$|B_\alpha| = p^{2k-2} + \left(\frac{\alpha \cdot \tilde{d}(A)}{p} \right) p^{k-1}.$$

This depends on the class of α in $\mathbb{F}_p/(\mathbb{F}_p^\times)^2 = \{\bar{0}, \bar{1}, \bar{\varepsilon}\}$ where $\varepsilon \in \mathbb{F}_p^\times$ is a nonsquare. If we write

$$S = \{(\mu, \lambda) \in \mathbb{F}_p \times \mathbb{F}_p \mid \mu - \lambda \in (\mathbb{F}_p^\times)^2\},$$

$$F = \sum_{(\mu, \lambda) \in S} \langle \mu, \lambda \rangle_U,$$

we obtain from (3.3) and (3.5)

$$\begin{aligned} G(A, O(A)) &= |B_0| \cdot G(U, O(U)) + |B_1| \cdot F + |B_\varepsilon| \cdot (-G(U, O(U)) - F) \\ &= (|B_0| - |B_\varepsilon|) \cdot G(U, O(U)) + (|B_1| - |B_\varepsilon|) \cdot F \\ &= \left(\frac{\tilde{d}(A)}{p} \right) p^{k-1} \cdot G(U, O(U)) + 2 \left(\frac{\tilde{d}(A)}{p} \right) p^{k-1} \cdot F. \end{aligned}$$

We shall show that

$$F = \begin{cases} 0, & p \equiv 3 \pmod{4}, \\ \left(\left(\frac{2\delta}{p} \right) \sqrt{p} - 1 \right) \cdot p, & p \equiv 1 \pmod{4}, \end{cases}$$

from which the proposition follows. In case $p \equiv 3 \pmod{4}$, since -1 is non-square, switching μ and λ gives

$$0 = \sum_{\mu, \lambda \in \mathbb{F}_p} \langle \mu, \lambda \rangle_U = G(U, O(U)) + \sum_{(\mu, \lambda) \in S} \langle \mu, \lambda \rangle_U + \sum_{(\lambda, \mu) \in S} \langle \mu, \lambda \rangle_U = 2F.$$

In case $p \equiv 1 \pmod{4}$, writing $\mu = \lambda + \alpha^2$ for $(\mu, \lambda) \in S$, we have

$$\begin{aligned} 2F &= \sum_{\lambda \in \mathbb{F}_p} \sum_{\alpha \in \mathbb{F}_p^\times} \langle \lambda + \alpha^2, \lambda \rangle_U \\ &= \sum_{\lambda \in \mathbb{F}_p} \sum_{v \in \mathbb{F}_p^\times} \zeta_p^{2^{-1}(\lambda v + \lambda v^{-1})} \sum_{\alpha \in \mathbb{F}_p^\times} \zeta_p^{2^{-1}v\alpha^2} \\ &= \sum_{v \in \mathbb{F}_p^\times} (G(A_{p, 2v}) - 1) \sum_{\lambda \in \mathbb{F}_p} \zeta_p^{2^{-1}\lambda(v + v^{-1})}. \end{aligned}$$

The square roots $\pm\delta$ of -1 are the solutions of $v + v^{-1} = 0$. We thus obtain

$$2F = 2p(G(A_{p, 2\delta}) - 1) = 2p \left(\left(\frac{2\delta}{p} \right) \sqrt{p} - 1 \right).$$

□

It remains to consider the anisotropic case. Since the 1-dimensional case is covered in §3.1, what remains is the anisotropic plane.

Proposition 3.4. *Let A be the anisotropic plane over \mathbb{F}_p with $p > 2$. Then $G(A, O(A)) = (-1)^{(p+1)/2} p$.*

Proof. Fix a nonsquare $\varepsilon \in \mathbb{F}_p^\times$. Since the scaling $A(\varepsilon)$ is isometric to A itself, there exists an isomorphism $j : A \rightarrow A$ of abelian groups such that $(j(x), j(y)) = \varepsilon(x, y)$ for every $x, y \in A$. For $\lambda \in \mathbb{F}_p^\times$ we write

$$A_\lambda^+ = \{(\lambda, x) | x \in A_{\lambda^2}\} \simeq A_{\lambda^2}, \quad A_\lambda^- = \{(\lambda, x) | x \in A_{\varepsilon\lambda^2}\} \simeq A_{\varepsilon\lambda^2},$$

and set

$$A^\pm = \bigsqcup_{\lambda \in \mathbb{F}_p^\times} A_\lambda^\pm, \quad \tilde{A} = A^+ \sqcup A^-.$$

\tilde{A} is a double covering of $A \setminus \{0\}$, with the covering transformation $(\lambda, x) \mapsto (-\lambda, x)$ which switches A_λ^\pm and $A_{-\lambda}^\pm$. On \tilde{A} we have an \mathbb{F}_p^\times -action defined by $\alpha \cdot (\lambda, x) = (\alpha\lambda, \alpha x)$. We can choose a reference point $(\lambda, x_\lambda^\pm) \in A_\lambda^\pm$ for each λ so that $x_{\alpha\lambda}^\pm = \alpha x_\lambda^\pm$ and $x_\lambda^- = j(x_\lambda^+)$. If we consider the mapping

$$\varphi : \tilde{A} \rightarrow \mathbb{F}_p, \quad A_\lambda^\pm \ni (\lambda, x) \mapsto (x_\lambda^\pm, x),$$

we have

$$2G(A, O(A)) = 2 + \sum_{(\lambda, x) \in \tilde{A}} \zeta_p^{\varphi(\lambda, x)}.$$

Claim 3.5. The fibers of φ over $\mathbb{F}_p^\times \subset \mathbb{F}_p$ have constant cardinality.

Proof. We let \mathbb{F}_p^\times act on \mathbb{F}_p by weight 2, i.e., $\alpha(t) = \alpha^2 t$. By our choice of x_λ^\pm , the map φ is \mathbb{F}_p^\times -equivariant. Hence its fibers have constant cardinality over $(\mathbb{F}_p^\times)^2$ and over $\varepsilon(\mathbb{F}_p^\times)^2$ respectively. We shall show that

$$(3.6) \quad |\varphi^{-1}((\mathbb{F}_p^\times)^2) \cap A^+| = |\varphi^{-1}(\varepsilon(\mathbb{F}_p^\times)^2) \cap A^+|,$$

which would then imply $|\varphi^{-1}((\mathbb{F}_p^\times)^2)| = |\varphi^{-1}(\varepsilon(\mathbb{F}_p^\times)^2)|$. We consider the map $j : A^+ \rightarrow A^-$ defined by $(\lambda, x) \mapsto (\lambda, j(x))$. Since $x_\lambda^- = j(x_\lambda^+)$, we have $\varphi(j(\lambda, x)) = \varepsilon \cdot \varphi(\lambda, x)$ for $(\lambda, x) \in A^+$. Hence

$$\begin{aligned} j(\varphi^{-1}((\mathbb{F}_p^\times)^2) \cap A^+) &\subset \varphi^{-1}(\varepsilon(\mathbb{F}_p^\times)^2) \cap A^-, \\ j(\varphi^{-1}(\varepsilon(\mathbb{F}_p^\times)^2) \cap A^+) &\subset \varphi^{-1}((\mathbb{F}_p^\times)^2) \cap A^-, \\ j(\varphi^{-1}(0) \cap A^+) &\subset \varphi^{-1}(0) \cap A^-. \end{aligned}$$

Since $j : A^+ \rightarrow A^-$ is bijective, the three inclusions are all equality. \square

By this claim we have

$$\begin{aligned} 2G(A, O(A)) &= 2 + |\varphi^{-1}(0)| + |\varphi^{-1}(1)| \sum_{\alpha \in \mathbb{F}_p^\times} \zeta_p^\alpha \\ &= 2 + |\varphi^{-1}(0)| - |\varphi^{-1}(1)| \\ &= -2p + \frac{p}{p-1} |\varphi^{-1}(0)|. \end{aligned}$$

In the last equality we used

$$(p-1)|\varphi^{-1}(1)| + |\varphi^{-1}(0)| = |\tilde{A}| = 2(p^2 - 1).$$

We are thus reduced to calculating $|\varphi^{-1}(0)|$.

For each $\lambda \neq 0$, $\varphi^{-1}(0) \cap A_\lambda^\pm$ is identified with the set of vectors in $(x_\lambda^\pm)^\perp \cap A$ having the same norm as x_λ^\pm . This set is non-empty if and only if $d(A) = -\varepsilon$ is a square, i.e., $\left(\frac{-1}{p}\right) = -1$. In that case it consists of two elements. It follows that

$$|\varphi^{-1}(0)| = \left(1 - \left(\frac{-1}{p}\right)\right) \cdot 2(p-1).$$

Therefore $G(A, O(A)) = -\left(\frac{-1}{p}\right)p$. \square

The above method can be extended to general p -elementary forms of even dimension. The result agrees with Proposition 3.3, of course.

3.3. Product formula. Let $p > 2$. Let A be the direct sum $A = A_{p^k, a} \oplus B$ where $k > 1$ and B is p -elementary. We show that a product formula holds for $G(A, O(A))$. This is not trivial as $O(A)$ does not preserve the decomposition in general. We first describe the orthogonal group $O(A)$, then classify the $O(A)$ -orbits, and finally calculate the Gauss sum.

Let e be the standard generator of $A_{p^k, a} \simeq \mathbb{Z}/p^k$. Using e , we can express an isomorphism $A \rightarrow A$ of abelian groups in the matrix form

$$(3.7) \quad \begin{pmatrix} x & p^{k-1}f \\ v & g \end{pmatrix} \in \begin{pmatrix} (\mathbb{Z}/p^k)^\times & p^{k-1}\text{Hom}(B, \mathbb{Z}/p) \\ B & \text{Hom}(B, B) \end{pmatrix}.$$

We define a subgroup of $O(A)$ isomorphic to $B \rtimes O(B)$ as follows. For $(v, g) \in B \rtimes O(B)$ we define $x_v \in (\mathbb{Z}/p^k)^\times$ and $f_{v,g} : B \rightarrow \mathbb{Z}/p$ by

$$x_v = 1 - 2^{-1}a^{-1}(p(v, v))p^{k-1},$$

$$f_{v,g}(?) = -a^{-1}p(g^{-1}(v), ?), \quad ? \in B,$$

where we view $p(v, v), p(g^{-1}(v), ?) \in \mathbb{Z}/p$. We define $\gamma_{v,g} : A \rightarrow A$ by

$$\gamma_{v,g} = \begin{pmatrix} x_v & p^{k-1}f_{v,g} \\ v & g \end{pmatrix}.$$

It is easy to check that $\gamma_{v,g}$ is an isometry and that the group

$$\Gamma = \{\gamma_{v,g} \mid (v, g) \in B \rtimes O(B)\}$$

is isomorphic to the semiproduct $B \rtimes O(B)$.

Proposition 3.6. *We have $O(A) = \{\pm 1\} \times \Gamma$.*

Proof. The isometry condition for the matrix (3.7) is

$$(3.8) \quad ax^2 + p^{k-1}(p(v, v)) \equiv a \pmod{p^k},$$

$$(3.9) \quad axf(?) + p(v, g(?)) = 0 \in \text{Hom}(B, \mathbb{Z}/p), \quad ? \in B, \\ g \in O(B).$$

The solutions of (3.8) are explicitly given by $x = \pm x_v$. Then f is uniquely determined from v, x and g by (3.9). \square

We consider the following subsets of A :

$$A_0 = ((\mathbb{Z}/p^k)^\times e) \times B, \quad A_1 = (p(\mathbb{Z}/p^{k-1})e) \times B.$$

We have $A = A_0 \cup A_1$. Each A_0, A_1 is preserved by $O(A)$.

Lemma 3.7. (1) The subset $((\mathbb{Z}/p^k)^\times e) \times \{0\}$ of A_0 is a representative for $\Gamma \backslash A_0$. For $x \in (\mathbb{Z}/p^k)^\times$ we have

$$(3.10) \quad \Gamma(xe) = \{x(x_v e + v) \mid v \in B\}.$$

(2) The Γ -orbit of $xe + w \in A_1$, where $x \in p(\mathbb{Z}/p^{k-1})$ and $w \in B$, is

$$\Gamma(xe + w) = \begin{cases} \{xe\}, & w = 0, \\ (x + p^{k-1}(\mathbb{Z}/p))e \times (O(B)w), & w \neq 0. \end{cases}$$

Proof. (1) Let $x \in (\mathbb{Z}/p^k)^\times$. The description (3.10) of the orbit is apparent. It implies that $x'e \notin \Gamma(xe)$ if $x \neq x' \in (\mathbb{Z}/p^k)^\times$. Since $|\Gamma(xe)| = |B|$, then $\Gamma((\mathbb{Z}/p^k)^\times e) = A_0$. The assertion (2) follows from

$$B(xe + w') = xe + B(w') = xe + w' + p^k(B, w')e$$

for $x \in p(\mathbb{Z}/p^{k-1})$ and $w' \in O(B)w \subset B$. \square

Before calculating $G(A, O(A))$, let us prepare a general formula.

Lemma 3.8. Let $p > 2$, $a \in \mathbb{Z}_p^\times$ and suppose that $k \geq 2$. Then

$$\sum_{x \in (\mathbb{Z}/p^k)^\times} \zeta_{p^k}^{ax^2} = 0.$$

Proof. If we write $S = ((\mathbb{Z}/p^k)^\times)^2 \subset \mathbb{Z}/p^k$, the right hand side is written as $2 \sum_{y \in S} \zeta_{p^k}^{ay}$. By the local square theorem, we have the additive action of $p(\mathbb{Z}/p^{k-1})$ on S . On each orbit, say $S_i = y_i + p(\mathbb{Z}/p^{k-1})$, we have

$$\sum_{y \in S_i} \zeta_{p^k}^{ay} = \sum_{y \in S_i} \zeta_{p^k}^{a(y+p)} = \zeta_{p^{k-1}}^a \cdot \sum_{y \in S_i} \zeta_{p^k}^{ay}.$$

Since $\zeta_{p^{k-1}}^a \neq 1$, this sum is equal to 0. \square

We are now ready to calculate the Gauss sum.

Proposition 3.9. *Let A be the direct sum $A = C \oplus B$ where $C = A_{p^k,a}$ with $p > 2, k > 1$ and B is p -elementary. Then*

$$G(A, O(A)) = G(C, O(C)) \cdot G(B, O(B)).$$

Proof. We take the sum over each stratum A_0, A_1 . We first consider A_0 . By Lemma 3.7 (1), we can take $((\mathbb{Z}/p^k)^\times / -1)e$ as reference points of $O(A) \setminus A_0$. For $x \in (\mathbb{Z}/p^k)^\times$ we have by (3.10)

$$\begin{aligned} (3.11) \quad \langle [xe], [xe] \rangle_A &= \sum_{v \in B} (\zeta_{p^k}^{ax^2 x_v} + \zeta_{p^k}^{-ax^2 x_v}) \\ &= 2\operatorname{Re} \left(\zeta_{p^k}^{ax^2} \cdot \sum_{v \in B} \zeta_p^{-2^{-1}x^2 p(v,v)} \right) \\ &= 2\operatorname{Re}(\zeta_{p^k}^{ax^2} \cdot G(B(-2))). \end{aligned}$$

Hence

$$\begin{aligned} \sum_{[y] \in O(A) \setminus A_0} \langle [y], [y] \rangle_A &= \frac{1}{2} \sum_{x \in (\mathbb{Z}/p^k)^\times} \langle [xe], [xe] \rangle_A \\ &= \operatorname{Re} \left(G(B(-2)) \sum_{x \in (\mathbb{Z}/p^k)^\times} \zeta_{p^k}^{ax^2} \right) = 0 \end{aligned}$$

by Lemma 3.8. We next consider the stratum A_1 . For $xe + w \in A_1$ we have

$$(3.12) \quad \langle [xe + w], [xe + w] \rangle_A = \begin{cases} \langle [xe], [xe] \rangle_C \cdot \langle [w], [w] \rangle_B, & w = 0, \\ p \cdot \langle [xe], [xe] \rangle_C \cdot \langle [w], [w] \rangle_B, & w \neq 0, \end{cases}$$

by Lemma 3.7 (2), where $[xe] \in C / -1$ and $[w] \in B / O(B)$. Since $\langle [x'e], [x'e] \rangle_C = \langle [xe], [xe] \rangle_C$ for $x' \in x + p^{k-1}(\mathbb{Z}/p)$, we have

$$\begin{aligned} \sum_{[y] \in O(A) \setminus A_1} \langle [y], [y] \rangle_A &= \sum_{[xe] \in pC / -1} \langle [xe], [xe] \rangle_C \cdot \sum_{[w] \in O(B) \setminus B} \langle [w], [w] \rangle_B \\ &= G(C, O(C)) \cdot G(B, O(B)). \end{aligned}$$

Here the second equality is a consequence of Lemma 3.8. \square

4. 2-ADIC CASE

In this section we study quadratic forms $A = (A, q)$ on 2-groups. Let $(,) : A \times A \rightarrow \mathbb{Q}/\mathbb{Z}$ be the associated bilinear form. For $x \in A$, $(x, x) = 2q(x)$ is well-defined as an element of $\mathbb{Q}/2\mathbb{Z}$, not just of \mathbb{Q}/\mathbb{Z} . We work with this refined symmetric bilinear form, from which the quadratic form q can be recovered. This is one of the differences with the case $p > 2$. Classification of quadratic forms on 2-groups is more complicated ([6]). Furthermore, the local square theorem is now $(\mathbb{Z}_2^\times)^2 = 1 + 8\mathbb{Z}_2$, hence $\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 = (\mathbb{Z}/8)^\times$.

Note also that the square x^2 of $x \in \mathbb{Z}/2^k$ can be defined as an element of $\mathbb{Z}/2^{k+1}$ and hence $x^2/2$ is well-defined as an element of $\frac{1}{2}\mathbb{Z}/2^k$.

For an odd number a we write $A_{2^k,a}$ for the quadratic form $(x, y) = axy/2^k$ on $\mathbb{Z}/2^k$. ($ax^2/2^k$ is considered as an element of $2^{-k}\mathbb{Z}/2\mathbb{Z}$ as noted above.) We denote by U, V the quadratic forms on $(\mathbb{Z}/2)^{\oplus 2}$ expressed by the Gram matrices

$$\begin{pmatrix} 0 & 2^{-1} \\ 2^{-1} & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2^{-1} \\ 2^{-1} & 1 \end{pmatrix} \quad \text{mod} \quad \begin{pmatrix} 2\mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & 2\mathbb{Z} \end{pmatrix}$$

respectively.

4.1. Cyclic forms.

Proposition 4.1. *Let $A = A_{2^k,a}$. When $k = 1$, we have $G(A, O(A)) = 0$. When $k > 1$, we have*

$$G(A, O(A)) = \left(\frac{2}{a}\right)^k \sqrt{|A|}.$$

Proof. The case $k = 1$ is clear. Let $k > 1$. We have $O(A) = \{\pm 1\}$, and -1 has two fixed points (the zero element and the unique order 2 element). Then

$$2G(A, O(A)) = 2 + 2 + \sum_{\substack{x \in \mathbb{Z}/2^k \\ 2x \neq 0}} (\zeta_{2^k}^{ax^2} + \zeta_{2^k}^{-ax^2}) = 2\text{Re}(G(A)).$$

We have $G(A) = \left(\frac{2}{a}\right)^k (1 + \sqrt{-1^a}) \sqrt{2^k}$ by [1] Proposition 1.5.3. \square

4.2. 2-elementary forms. Let A be a quadratic form on a 2-elementary group. By the nondegeneracy there exists a unique element $x_A \in A$ such that $(x, x_A) = (x, x) \bmod \mathbb{Z}$ for every $x \in A$. This element x_A is called the *characteristic element* of A . We denote $A_+ = x_A^\perp$, the group of elements of A whose norm is in \mathbb{Z} . When $x_A = 0$, namely $A = A_+$, then A is said to be *special*. In that case we have $A \simeq U^m$ or $A \simeq U^{m-1} \oplus V$. We set δ_A by $\delta_A = 1$ in the first case and $\delta_A = -1$ in the second case. When A is non-special, it is isometric to $A' \oplus A''$ where A' is special and $A'' \simeq (A_{2,1})^i \oplus (A_{2,-1})^j$ with $1 \leq i + j \leq 2$ (see [6]). When $i + j = 1$, x_A is the generator of A'' . When $i + j = 2$, x_A is the unique nonzero element of A'' with $(x_A, x_A) \in \mathbb{Z}$, and generates the radical of A_+ .

By definition the characteristic element x_A is invariant under the action of $O(A)$. Except this, description of $O(A)$ -orbits is the same as the nondyadic case. We use the following 2-adic versions of Witt cancelation.

Lemma 4.2. (1) *Let A be a 2-elementary form and $A_1, A_2 \subset A$ be nondegenerate special forms. If $A_1 \simeq A_2$, then $A_1^\perp \simeq A_2^\perp$. In particular, there exists an isometry $A \rightarrow A$ which maps A_1 to A_2 .*

(2) Let A_1, A_2 be non-special 2-elementary forms and let $a = 1$ or -1 . If $A_1 \oplus A_{2,a} \simeq A_2 \oplus A_{2,a}$, then $A_1 \simeq A_2$.

Proof. The assertion (1) is proved in [5] Proposition 1.5. We consider (2) in case $\dim(A_1) = \dim(A_2)$ is odd. Using (1) for $U^k \hookrightarrow A_i$, we may assume that A_1 and A_2 are one of

$$U \oplus A_{2,1}, \quad U \oplus A_{2,-1}, \quad V \oplus A_{2,1}, \quad V \oplus A_{2,-1}.$$

When $A_1 \neq A_2$, we see that $A_1 \oplus A_{2,a}$ and $A_2 \oplus A_{2,a}$ have different representation numbers by direct calculation, hence cannot be isometric. The case $\dim(A_1) = \dim(A_2)$ even is similar. \square

Proposition 4.3. *Let A be a finite quadratic form on a 2-elementary group and $x, y \in A$ be nonzero, non-characteristic elements. The elements x and y are $O(A)$ -equivalent if and only if they have the same norm in $\mathbb{Q}/2\mathbb{Z}$.*

Proof. It suffices to prove the "if" direction. We first consider the case $(x, x) \notin \mathbb{Z}$. Since $\langle x \rangle$ and $\langle y \rangle$ are nondegenerate, we have the orthogonal decomposition $A = \langle x \rangle \oplus x^\perp = \langle y \rangle \oplus y^\perp$. Since x and y are non-characteristic, x^\perp and y^\perp are non-special. Then $x^\perp \simeq y^\perp$ by Lemma 4.2 (2), so x and y are $O(A)$ -equivalent.

Next let $(x, x) \in \mathbb{Z}$. We assume $A_+/\text{rad}(A_+) \neq V$: this exceptional case can be treated directly. We shall show that there exists an embedding $U \hookrightarrow A$ whose image contains x . The same also applies to y , and then our assertion follows from Lemma 4.2 (1). Now since x is nonzero and non-characteristic, it is not contained in the radical of A_+ . Hence we can find an element $x' \in A_+$ such that $(x, x') = 1/2$. If either x or x' has norm 0, then $\langle x, x' \rangle \simeq U$. If both x and x' have norm 1, then $\langle x, x' \rangle \simeq V$. By our assumption $\langle x, x' \rangle^\perp \cap A_+$ contains U or V , so it contains a norm 1 vector x'' . Then $\langle x, x' + x'' \rangle \simeq U$. \square

For $\mu \in 2^{-1}\mathbb{Z}/2\mathbb{Z}$ we write $A_\mu \subset A$ for the subset of vectors of norm μ . Then the $O(A)$ -orbit decomposition of A is

$$A = \{0\} \cup \{x_A\} \cup \bigcup_{\mu \in 2^{-1}\mathbb{Z}/2\mathbb{Z}} (A_\mu \setminus \{0, x_A\}).$$

We first consider the case A contains U .

Proposition 4.4. *Let A be a 2-elementary form that contains U . Then*

$$G(A, O(A)) = \begin{cases} \delta_A \sqrt{|A|}, & A : \text{special}, \\ 0, & A : \text{non-special}. \end{cases}$$

Proof. We write $A = U \oplus B$ and let u_1, u_2 be the standard basis of U . In case A is non-special, we can also write $A = A_{2,1} \oplus A_{2,-1} \oplus C$ because $U \oplus A_{2,\pm 1} \simeq (A_{2,\pm 1})^2 \oplus A_{2,\mp 1}$. We denote by u_\pm the generator of $A_{2,\pm 1}$. As a

reference vector in A_μ we can take $x_\mu = u_1, u_1 + u_2, u_\pm$ for $\mu = 0, 1, \pm 1/2$ respectively. We have the simple expression

$$(4.1) \quad G(A, O(A)) = \sum_{\mu \in 2^{-1}\mathbb{Z}/2\mathbb{Z}} \sum_{x \in A_\mu} e((x_\mu, x))$$

because $(x_\lambda, x_A) = (x_A, x_A)$ for $\lambda = (x_A, x_A)$. Since we have the partitions

$$\begin{aligned} A_\mu &= \{0, u_1, u_2\} \times B_\mu \sqcup \{u_1 + u_2\} \times B_{1-\mu}, \quad \mu = 0, 1, \\ A_{\pm 1/2} &= \{u_\pm\} \times C_0 \sqcup \{u_\mp\} \times C_1 \sqcup \{0, u_+ + u_-\} \times C_{\pm 1/2}, \end{aligned}$$

we obtain

$$(4.2) \quad \sum_{x \in A_0} e((u_1, x)) = \sum_{x \in A_1} e((u_1 + u_2, x)) = |B_0| - |B_1|,$$

$$(4.3) \quad \sum_{x \in A_{\pm 1/2}} e((u_\pm, x)) = |C_1| - |C_0|.$$

Similarly, we have

$$\begin{aligned} |A_0| &= 3|B_0| + |B_1| = 2|C_0| + |C_{1/2}| + |C_{-1/2}|, \\ |A_1| &= |B_0| + 3|B_1| = 2|C_1| + |C_{1/2}| + |C_{-1/2}|, \end{aligned}$$

and hence

$$|A_0| - |A_1| = 2(|B_0| - |B_1|) = 2(|C_0| - |C_1|).$$

Hence $G(A, O(A)) = 0$ when A is non-special, and $G(A, O(A)) = |A_0| - |A_1|$ when A is special. In the latter case we have $|A_0| - |A_1| = \delta_A \sqrt{|A|}$ by induction on $\dim(A)/2$. \square

The remaining cases are covered by the following.

Proposition 4.5. *We have*

$$G(A, O(A)) = \begin{cases} 0, & A = V, A_{2,1} \oplus A_{2,-1}, (A_{2,a})^3, \\ \sqrt{|A|}, & A = (A_{2,a})^2, (A_{2,a})^4. \end{cases}$$

Proof. This can be checked directly. \square

4.3. Product formula. Let A be the direct sum $A = A_{2^k,a} \oplus B$ such that $k \geq 2$ and B is 2-elementary. We show that a product formula like Proposition 3.9 holds when $k \geq 4$, but not always when $k \leq 3$. As in (3.7), we express an isomorphism $A \rightarrow A$ in the form $\begin{pmatrix} x & 2^{k-1}f \\ v & g \end{pmatrix}$. The isometry condition is

$$(4.4) \quad x^2 \equiv 1 - 2^{k-1} \cdot a(2(v, v)) \pmod{2^{k+1}},$$

$$(4.5) \quad f(?) \equiv 2(v, g(?)) \pmod{2}, \quad ? \in B,$$

$$(4.6) \quad (g(?), g(?)) \equiv (?, ?) - f(?) \cdot 2^{k-2} \pmod{2\mathbb{Z}}, \quad ? \in B,$$

where $2(v, v) \in \mathbb{Z}/4$ and $2(v, g(?)), f(?) \in \mathbb{Z}/2$. The condition (4.6) becomes $g \in O(B)$ when $k \geq 3$. When $k \geq 4$, the equation (4.4) always has two solutions, one of which is given by

$$x_v = \begin{cases} 1 - 2^{k-2}a(2(v, v)), & k \geq 5, \\ 1 + 4a(2(v, v)), & k = 4. \end{cases}$$

In case $k = 3$, by the local square theorem, (4.4) has a solution if and only if $(v, v) \in \mathbb{Z}$. In that case, a solution is given by $x_v = 1 + 4(v, v)$.

Let $k \geq 4$. For $(v, g) \in B \rtimes O(B)$ we define the isometry $\gamma_{v,g}$ of A by $\gamma_{v,g} = \begin{pmatrix} x_v & 2^{k-1}f_{v,g} \\ v & g \end{pmatrix}$ where $f_{v,g}$ is defined from v and g by (4.5). We put

$$(4.7) \quad \Gamma = \{\gamma_{v,g} \mid (v, g) \in B \rtimes O(B)\}.$$

We have $O(A) = \{\pm 1\} \times \Gamma$ by the same argument as in Proposition 3.6, and the assertion of Lemma 3.7 still holds. Also Lemma 3.8 holds in $k \geq 4$ by the local square theorem in $p = 2$:

$$\sum_{x \in (\mathbb{Z}/2^k)^\times} \zeta_{2^k}^{ax^2} = 0, \quad k \geq 4.$$

Hence the argument of §3.3 works in $p = 2, k \geq 4$:

Proposition 4.6. *Let A be the direct sum $A = C \oplus B$ such that $C = A_{2^k,a}$ with $k \geq 4$ and B is 2-elementary. Then*

$$G(A, O(A)) = G(C, O(C)) \cdot G(B, O(B)).$$

We consider the case $k = 2, 3$.

Proposition 4.7. *Let $A = C \oplus B$ where $C = A_{8,a}$ and B is 2-elementary. Then*

$$G(A, O(A)) = \begin{cases} 0, & B : \text{non-special}, \\ G(C, O(C)) \cdot G(B, O(B)), & B : \text{special}, \\ -2G(C, O(C)), & B = V. \end{cases}$$

By §4.2, the product formula does not hold when $B = V, (A_{2,a})^2, (A_{2,a})^4$.

Proof. We replace (4.7) by the group $\Gamma_+ = B_+ \rtimes O(B)$ where $B_+ \subset B$ is the subgroup of elements of norm $\in \mathbb{Z}$. Then $O(A) = \{\pm 1\} \times \Gamma_+$. Let

$$A_{0+} = ((\mathbb{Z}/8)^\times e) \times B_+, \quad A_{0-} = ((\mathbb{Z}/8)^\times e) \times (B \setminus B_+), \quad A_1 = (2(\mathbb{Z}/4)e) \times B,$$

which are preserved by $O(A)$. If $xe + w \in A_1$, then

$$O(A)(xe + w) = (\pm x + 4(2(B_+, w)))e \times O(B)w,$$

where $2(B_+, w)$ is a subgroup of $\mathbb{Z}/2\mathbb{Z}$. Hence we have

$$\sum_{[y] \in \mathcal{O}(A) \setminus A_1} \langle [y], [y] \rangle_A = \left(\sum_{z \in 2C/-1} \langle [z], [z] \rangle_C \right) \cdot G(B, \mathcal{O}(B)) = 0,$$

where $\sum_{2C/-1} \langle [z], [z] \rangle_C = 0$ by direct calculation. For A_{0+} , the coset $\mathcal{O}(A) \setminus A_{0+}$ consists of $[e]$ and $[3e]$. Since

$$\mathcal{O}(A)(xe) = \{\pm(x + 4(v, v))e + v \mid v \in B_+\}$$

for $x = 1, 3$, we obtain

$$\sum_{[y] \in \mathcal{O}(A) \setminus A_{0+}} \langle [y], [y] \rangle = 2(\zeta_8^a + \zeta_8^{-a}) \sum_{v \in B_+} (-1)^{(v, v)} = G(C, \mathcal{O}(C)) \cdot (|B_0| - |B_1|).$$

As shown in the proof of Proposition 4.4, we have $|B_0| - |B_1| = G(B, \mathcal{O}(B))$ when B is special and $B \neq V$, which proves the proposition in this case. The case $B = V$ is immediate. Suppose that B is non-special. If we choose $w_0 \in B \setminus B_+$, then $\mathcal{O}(A) \setminus A_{0-}$ consists of $[e + w_0]$ and $[3e + w_0]$. For $x = 1, 3$ we have

$$\mathcal{O}(A)(xe + w_0) = \{\pm(x + 4((w, w) - (w_0, w_0)))e + w \mid w \in B \setminus B_+\}.$$

It follows that

$$\begin{aligned} \langle [xe + w_0], [xe + w_0] \rangle_A &= (\zeta_8^a + \zeta_8^{-a}) \sum_{w \in B \setminus B_+} (-1)^{(w, w) - (w_0, w_0) + 2(w_0, w)} \\ &= -(\zeta_8^a + \zeta_8^{-a}) \sum_{v \in B_+} (-1)^{(v, v)} = -\langle [xe], [xe] \rangle_A. \end{aligned}$$

Therefore $G(A, \mathcal{O}(A)) = 0$ in this case. \square

Proposition 4.8. *Let $A = A_{4,a} \oplus B$ where B is 2-elementary. Then*

$$G(A, \mathcal{O}(A)) = \begin{cases} 4, & B = (A_{2,a})^2, A_{2,1} \oplus A_{2,-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $x \in A$ is of order 4, then for all $y \in \mathcal{O}(A)x$ we have $(x, y) \equiv \pm 1/4 \pmod{\mathbb{Z}}$ and $y \neq -y$. Then

$$\langle [x], [x] \rangle_A = \sum_{y \in \mathcal{O}(A)x/\pm 1} e((x, y)) + e((x, -y)) = \sum_y (\sqrt{-1} - \sqrt{-1}) = 0,$$

hence $G(A, \mathcal{O}(A))$ reduces to

$$G(A, \mathcal{O}(A)) = \sum_{\substack{[x] \in \mathcal{O}(A) \setminus A \\ 2x=0}} \langle [x], [x] \rangle_A.$$

When $B = A_{2,1} \oplus A_{2,-1}$, the assertion follows by direct calculation. When B is anisotropic, the decomposition $A = A_{4,a} \oplus B$ is canonical, so the assertion follows from Lemma 2.1 and the results of §4.1 and §4.2. We

consider the general case $B = B' \oplus B''$ where $B' \neq 0$ is special and $B'' = (A_{2,1})^i \oplus (A_{2,-1})^j$ with $0 \leq i + j \leq 2$. We will show that $G(A, O(A)) = 0$ in this case. Let $x_B \in B''$ be the characteristic element of B . Let $e \in A_{4,a}$ be a generator. We have the exceptional elements $0, 2e, x_B, 2e + x_B$ fixed by $O(A)$. (x_B can be 0.) Extending Lemma 4.3, we can show that other two elements of order 2 in A are $O(A)$ -equivalent if and only if they have the same norm. The possibilities for x_B are: (1) $x_B = 0$, (2) $x_B \neq 0, (x_B, x_B) = 0$, (3) $(x_B, x_B) = 1$, and (4) $(x_B, x_B) = \pm 1/2$.

We consider only the case (2): other cases can be calculated similarly. If $x \in A$ has norm 0 with $x \neq 0, x_B$, then

$$O(A)x = \{y \in B \mid (y, y) = 0, y \neq 0, x_B\} \sqcup \{y + 2e \mid y \in B, (y, y) = 1\}.$$

Hence

$$(4.8) \quad \langle [x], [x] \rangle_A = \sum_{\substack{y \in B+ \\ y \neq 0, x_B}} e((x, y)) = -2.$$

Similarly, for other orbits $[x]$, we have

$$(4.9) \quad \langle [x], [x] \rangle_A = \begin{cases} -2, & (x, x) = 1, x \neq 2e, 2e + x_B, \\ 0, & (x, x) = \pm 1/2. \end{cases}$$

The contribution from the exceptional orbits $0, 2e, x_B, 2e + x_B$ is $1 + 1 + 1 + 1 = 4$, hence $G(A, O(A)) = 0$. \square

5. EQUIVARIANT GAUSS SUM OF THE SECOND KIND

In this section we evaluate the equivariant Gauss sum $G'(A, O(A))$ of the second kind for quadratic forms A as in the previous sections. Some part is similar to the case of $G(A, O(A))$, so we omit the detail there.

5.1. Cyclic forms.

Proposition 5.1. *Let $A = A_{p^k, a}$ with $p \geq 2$ and $a \in \mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2$.*

(1) *If $p > 3$, then*

$$G'(A, O(A)) = \frac{1}{2} \left(1 + \left(\frac{p}{3} \right)^k \right) \left(\frac{2a}{p} \right)^k \sqrt{|A|} \times \begin{cases} 1, & p^k \equiv 1 \pmod{4}, \\ \sqrt{-1}, & p^k \equiv 3 \pmod{4}. \end{cases}$$

(2) *For $p = 2, 3$ we have*

$$G'(A, O(A)) = \begin{cases} -\sqrt{-1}^{k^2} \left(\frac{-a}{3} \right)^k \zeta_3^{-a} \sqrt{|A|}, & p = 3, \\ \frac{1}{2} (1 + (-1)^{k+1}) \left(\frac{2}{a} \right)^{k+1} \zeta_8^{-1} \zeta_4^{(a+1)^2/4} \sqrt{|A|}, & p = 2. \end{cases}$$

Proof. When $p > 2$, we have

$$\begin{aligned} G'(A, O(A)) &= 1 + \frac{1}{2} \sum_{\substack{x \in \mathbb{Z}/p^k \\ x \neq 0}} \zeta_{p^k}^{-2^{-1}ax^2} (\zeta_{p^k}^{ax^2} + \zeta_{p^k}^{-ax^2}) \\ &= \frac{1}{2} \{G(A(2)) + G(A(-6))\}. \end{aligned}$$

When $p > 3$, the assertion follows from the formula of $G(A(\varepsilon))$ ([1] Theorem 1.5.2) and the quadratic reciprocity $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. When $p = 3$, $A(-6) \simeq A(3)$ is degenerate with kernel $3^{k-1}A \simeq \mathbb{Z}/3$, so we have

$$\begin{aligned} G'(A, O(A)) &= \frac{1}{2} (G(A(-1)) + 3G(A_{3^{k-1},a})) \\ &= \frac{1}{2} \cdot \left(\frac{-a}{3}\right)^k \cdot \sqrt{3^k} \cdot \left\{ \sqrt{-1}^{k^2} + \sqrt{3} \left(\frac{-1}{3}\right)^k \left(\frac{a}{3}\right) \sqrt{-1}^{(k-1)^2} \right\} \\ &= \left(\frac{-a}{3}\right)^k \sqrt{-1}^{k^2} \sqrt{3^k} \cdot \frac{1}{2} \left(1 + \left(\frac{a}{3}\right) \sqrt{-3}\right). \end{aligned}$$

When $p = 2$, $k \geq 3$, we have

$$\begin{aligned} G'(A, O(A)) &= 1 + 1 + \frac{1}{2} \sum_{\substack{x \in \mathbb{Z}/2^k \\ 2x \neq 0}} (\zeta_{2^{k+1}}^{ax^2} + \zeta_{2^{k+1}}^{-3ax^2}) \\ &= \frac{1}{4} \{G(A_{2^{k+1},a}) + G(A_{2^{k+1},-3a})\} \\ &= \frac{1}{4} \left(\left(\frac{2}{a}\right)^{k+1} + \left(\frac{2}{-3a}\right)^{k+1} \right) \cdot (1 + \sqrt{-1}^a) \cdot \sqrt{2^{k+1}}. \end{aligned}$$

The case $p = 2$, $k \leq 2$ can be calculated directly. \square

5.2. p -elementary forms. We first consider the case $p > 2$. We begin with the hyperbolic plane U .

Lemma 5.2. *Let $p > 2$. We have $G'(U, O(U)) = \left(1 + \left(\frac{p}{3}\right)\right)p$.*

Proof. As in (3.2) we have

$$G'(U, O(U)) = \sum_{\mu \in \mathbb{F}_p} \zeta_p^{-2^{-1}\mu} \langle \mu, \mu \rangle_U = \sum_{\nu \in \mathbb{F}_p^\times} \sum_{\mu \in \mathbb{F}_p} \zeta_p^{2^{-1}\mu(-1+\nu+\nu^{-1})}.$$

When $p \neq 3$, the equation $-1 + \nu + \nu^{-1} = 0$ has (two) solutions in \mathbb{F}_p^\times if and only if $\left(\frac{-3}{p}\right) = 1$, and we have $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. When $p = 3$, this equation has the unique solution $\nu = -1$. \square

Proposition 5.3. *Let A be a quadratic space over \mathbb{F}_p with $p > 2$ of dimension m and discriminant $d(A)$. We write $k = [m/2]$. When $p \equiv 1 \pmod{3}$, choose a solution $\delta \in \mathbb{F}_p$ of $\delta^2 - \delta + 1 = 0$. (δ is a primitive 6-th root of 1 in \mathbb{F}_p .)*

1) *When A contains an isotropic vector, then*

$$G'(A, O(A)) = \begin{cases} 0, & p \equiv 2 \pmod{3}, \\ 2\zeta_{16}^{m^2(p-1)^2} \left(\frac{2\delta}{p}\right)^m \left(\frac{(-1)^k d(A)}{p}\right) \sqrt{|A|}, & p \equiv 1 \pmod{3}, \\ (\sqrt{-1})^{-m} \left(\frac{d(A)}{3}\right) \sqrt{|A|}, & p = 3. \end{cases}$$

(2) *When A is the anisotropic plane, then $G'(A, O(A)) = -\left(\frac{p}{3}\right)p$.*

Proof. (1) We reuse the notation in the proof of Proposition 3.3. When $m = 2k$ is even, we have as in (3.3) and (3.5)

$$\begin{aligned} G'(A, O(A)) &= \sum_{\mu, \lambda \in \mathbb{F}_p} \zeta_p^{-2^{-1}\mu} \cdot |B_{\mu-\lambda}| \cdot \langle \mu, \lambda \rangle_U \\ &= |B_0| \cdot G'(U, O(U)) + |B_1| \cdot \sum_{\mu \neq \lambda} \zeta_p^{-2^{-1}\mu} \cdot \langle \mu, \lambda \rangle_U \\ &= (|B_0| - |B_1|) \cdot G'(U, O(U)) \\ &= \delta_A \cdot p^{k-1} \cdot G'(U, O(U)). \end{aligned}$$

In the third equality we used $\sum_{\mu, \lambda} \zeta_p^{-2^{-1}\mu} \langle \mu, \lambda \rangle_U = 0$. The proposition follows from Lemma 5.2.

Next let $m = 2k + 1$ be odd. We set

$$F' = \sum_{(\mu, \lambda) \in S} \zeta_p^{-2^{-1}\mu} \langle \mu, \lambda \rangle_U.$$

Then $G'(A, O(A))$ is given by

$$\begin{aligned} &|B_0| \cdot G'(U, O(U)) + |B_1| \cdot F' - |B_\varepsilon| \cdot (G'(U, O(U)) + F') \\ &= \left(\frac{\tilde{d}(A)}{p}\right) p^{k-1} \cdot G'(U, O(U)) + 2 \left(\frac{\tilde{d}(A)}{p}\right) p^{k-1} \cdot F'. \end{aligned}$$

So it suffices to calculate F' . We have

$$\begin{aligned} 2F' &= \sum_{\mu \in \mathbb{F}_p} \sum_{\alpha \in \mathbb{F}_p^\times} \sum_{v \in \mathbb{F}_p^\times} \zeta_p^{2^{-1}\mu(-1+v+v^{-1})-2^{-1}\alpha^2 v^{-1}} \\ &= \sum_{v \in \mathbb{F}_p^\times} \left(\sum_{\mu \in \mathbb{F}_p} \zeta_p^{2^{-1}\mu(-1+v+v^{-1})} \right) \cdot (G(A_{p,-2v}) - 1). \end{aligned}$$

When $p \equiv 2 \pmod{3}$, we have $v + v^{-1} \neq 1$ for any $v \in \mathbb{F}_p^\times$ so that $F' = 0$. When $p \equiv 1 \pmod{3}$, we have two solutions δ, δ^{-1} of $v + v^{-1} = 1$. Then $F' = p(G(A_{p,-2\delta}) - 1)$. Finally, when $p = 3$, $v + v^{-1} = 1$ has the unique solution

$\nu = -1$ and thus $2F' = 3(G(A_{3,-1}) - 1)$. It is now straightforward to finish the calculation of $G'(A, O(A))$.

(2) We keep the notation in the proof of Proposition 3.4. Instead of φ , we consider the map

$$\varphi' : \tilde{A} \rightarrow \mathbb{F}_p, \quad A_\lambda^\pm \ni (\lambda, x) \mapsto (x_\lambda^\pm, x) - (x_\lambda^\pm, x_\lambda^\pm)/2.$$

Then

$$2G'(A, O(A)) = 2 + \sum_{(\lambda, x) \in \tilde{A}} \zeta_p^{\varphi'(\lambda, x)}.$$

As in Claim 3.5, φ' has constant fiber cardinality over $\mathbb{F}_p^\times \subset \mathbb{F}_p$. Hence

$$2G'(A, O(A)) = 2 + |(\varphi')^{-1}(0)| - |(\varphi')^{-1}(1)| = -2p + \frac{p}{p-1}|(\varphi')^{-1}(0)|.$$

If $\varphi'(\lambda, x) = 0$, we can write $x = (x_\lambda^\pm + y)/2$ for some $y \in (x_\lambda^\pm)^\perp$. Hence

$$(\varphi')^{-1}(0) \cap A_\lambda^\pm \simeq \{y \in (x_\lambda^\pm)^\perp \mid (y, y) = 3(x_\lambda^\pm, x_\lambda^\pm)\}.$$

When $p > 3$, this set is non-empty (consisting of two points) if and only if $3 \in d(A) \cdot (\mathbb{F}_p^\times)^2$, namely -3 is nonsquare. It follows that

$$|(\varphi')^{-1}(0)| = \left(1 - \left(\frac{p}{3}\right)\right) \cdot 2(p-1).$$

When $p = 3$, $(\varphi')^{-1}(0) \cap A_\lambda^\pm$ consists of one point and hence $|(\varphi')^{-1}(0)| = 2(p-1)$. \square

Proposition 5.4. *Let A be a 2-elementary form of dimension $m > 1$. Then*

$$G'(A, O(A)) = \begin{cases} 0, & A \text{ contains } U \text{ or } A = (A_{2,a})^2, \\ \sqrt{|A|}, & A = V, A_{2,1} \oplus A_{2,-1}, (A_{2,a})^4, \\ 2(1 + \sqrt{-1}^{-a}), & A = (A_{2,a})^3. \end{cases}$$

Proof. The exceptional cases can be checked directly. Let A contain U . We have as in (4.1)

$$G'(A, O(A)) = \sum_{\mu \in 2^{-1}\mathbb{Z}/2\mathbb{Z}} \sqrt{-1}^{-2\mu} \sum_{x \in A_\mu} e((x_\mu, x)).$$

By (4.2) and (4.3) we obtain $G'(A, O(A)) = 0$. \square

5.3. Product formula.

Proposition 5.5. *Let $p \geq 2$ and A be the direct sum $A = C \oplus B$ where $C = A_{p^k,a}$ with $k > 1$ and B is p -elementary. Then*

$$G'(A, O(A)) = G'(C, O(C)) \cdot G'(B, O(B)).$$

Proof. We first consider the case $p > 2$. We use the notation in §3.3. For $[xe] \in \mathcal{O}(A) \setminus A_0$, $x \in (\mathbb{Z}/p^k)^\times$, we have by (3.11)

$$e(-q(xe))\langle [xe], [xe] \rangle_A = \zeta_{p^k}^{2^{-1}ax^2} G(B(-2)) + \zeta_{p^k}^{-2^{-1} \cdot 3ax^2} G(B(2)).$$

If $p > 3$, we obtain

$$\sum_{[y] \in \mathcal{O}(A) \setminus A_0} e(-q(y))\langle [y], [y] \rangle_A = 0.$$

by Lemma 3.8. When $p = 3$, we have

$$\sum_{[y] \in \mathcal{O}(A) \setminus A_0} e(-q(y))\langle [y], [y] \rangle_A = G(B(2)) \cdot \frac{3}{2} \sum_{x \in (\mathbb{Z}/3^{k-1})^\times} \zeta_{3^{k-1}}^{-2^{-1}ax^2}.$$

This is equal to 0 when $k > 2$, and to $G(B(2)) \cdot 3\zeta_3^a$ when $k = 2$. For the stratum A_1 we have by (3.12)

$$\begin{aligned} & \sum_{[y] \in \mathcal{O}(A) \setminus A_1} e(-q(y))\langle [y], [y] \rangle_A \\ &= \left(\sum_{[xe] \in pC/-1} e(-q(xe))\langle [xe], [xe] \rangle_C \right) \cdot \left(\sum_{[w] \in \mathcal{O}(B) \setminus B} e(-q(w))\langle [w], [w] \rangle_B \right). \end{aligned}$$

The second term is $G'(B, \mathcal{O}(B))$. When $(p, k) \neq (3, 2)$, the first term is equal to $G'(C, \mathcal{O}(C))$ by Lemma 3.8. Let $(p, k) = (3, 2)$. Then the first term is equals to 3. If B contains U , we may use Proposition 5.3 to obtain

$$\begin{aligned} G'(A, \mathcal{O}(A)) &= 3 \sqrt{-1}^{-m} \left(\frac{d(B)}{3} \right) \sqrt{|B|} \cdot (1 + \zeta_3^a) \\ &= G'(C, \mathcal{O}(C)) \cdot G'(B, \mathcal{O}(B)). \end{aligned}$$

If B is anisotropic, the decomposition $A = C \oplus B$ is canonical and we can use Lemma 2.1.

Next let $p = 2$. When $k \geq 4$, the above calculation is still valid. When $k = 3$, we have as in the proof of Proposition 4.7

$$\begin{aligned} & \sum_{[x] \in \mathcal{O}(A) \setminus A_1} e(-q(x))\langle [x], [x] \rangle = G'(C, \mathcal{O}(C)) \cdot G'(B, \mathcal{O}(B)), \\ & \sum_{[x] \in \mathcal{O}(A) \setminus A_{0+}} e(-q(x))\langle [x], [x] \rangle = (\zeta_{16}^a + \zeta_{16}^{5a} + \zeta_{16}^{9a} + \zeta_{16}^{13a}) \sum_{v \in B_+} (-1)^{(v,v)} = 0, \end{aligned}$$

and similarly $\sum_{[x] \in \mathcal{O}(A) \setminus A_{0-}} e(-q(x))\langle [x], [x] \rangle = 0$. When $k = 2$, we have $G'(C, \mathcal{O}(C)) = 0$ by Proposition 5.1. We shall show that $G'(A, \mathcal{O}(A)) = 0$. As in the proof of Proposition 4.8, $G'(A, \mathcal{O}(A))$ can be reduced to

$$G(A, \mathcal{O}(A)) = \sum_{\substack{[x] \in \mathcal{O}(A) \setminus A \\ 2x=0}} e(-q(x))\langle [x], [x] \rangle_A,$$

and we may assume that $B' \neq 0$. When x_B is nonzero and isotropic, (4.8) and (4.9) show that the contribution from orbits other than 0 , x_B , $2e$ and $x_B + 2e$ cancels to 0 . The contribution from those elements also amounts to 0 , so we have $G'(A, O(A)) = 0$. The case of other x_B is similar. \square

Remark 5.6. We also checked that $G'(A, O(A)) = 0$ for $A = A_{2^k, a} \oplus A_{4, b}$ and $A = A_{2^k, a} \oplus A_{4, b} \oplus A_{2, c}$ where $k \geq 2$. Since $G'(A_{4, b}, O(A_{4, b})) = 0$ by Proposition 5.1, the product formula also holds in this case.

6. MODULAR FORMS FOR THE WEIL REPRESENTATION

In this section we explain that the equivariant Gauss sums $G(A, O(A))$ and $G'(A, O(A))$ appear in the dimension formula for certain vector-valued modular forms. This was our original motivation to study them.

Let $A = (A, q)$ be a finite quadratic form. We write $\sigma(A) \in \mathbb{Z}/8$ for its signature. We recall the Weil representation associated to A (see [2]). Let $\text{Mp}_2(\mathbb{Z})$ be the metaplectic double cover of $\text{SL}_2(\mathbb{Z})$. Its elements are pairs $(M, \phi(\tau))$ where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and $\phi(\tau)$ is a holomorphic function on the upper half plane such that $\phi(\tau)^2 = c\tau + d$. The group $\text{Mp}_2(\mathbb{Z})$ is generated by the elements

$$T = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, 1 \right), \quad S = \left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sqrt{\tau} \right).$$

Its center is cyclic of order 4 generated by

$$Z = S^2 = \left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \sqrt{-1} \right).$$

Let $\mathbb{C}A$ be the group algebra over A . We denote by $\mathbf{e}_x \in \mathbb{C}A$ the standard basis vector corresponding to $x \in A$. The Weil representation ρ_A is the unitary representation of $\text{Mp}_2(\mathbb{Z})$ on $\mathbb{C}A$ defined by

$$\begin{aligned} \rho_A(T)(\mathbf{e}_x) &= e(q(x))\mathbf{e}_x, \\ \rho_A(S)(\mathbf{e}_x) &= \frac{\zeta_8^{-\sigma(A)}}{\sqrt{|A|}} \sum_{y \in A} e(-(x, y))\mathbf{e}_y. \end{aligned}$$

The orthogonal group $O(A) = O(A, q)$ acts on $\mathbb{C}A$ by permuting the basis vectors \mathbf{e}_x , namely $\gamma(\mathbf{e}_x) = \mathbf{e}_{\gamma x}$ for $\gamma \in O(A)$. This action commutes with ρ_A :

$$\rho_A(T) \circ \gamma = \gamma \circ \rho_A(T), \quad \rho_A(S) \circ \gamma = \gamma \circ \rho_A(S).$$

Let $l \in \frac{1}{2}\mathbb{Z}$. A $\mathbb{C}A$ -valued holomorphic function $f(\tau)$ on the upper half plane is called a modular form of type ρ_A and weight l if it satisfies

$$f(M\tau) = \rho_A(M, \phi)\phi(\tau)^{2l}f(\tau), \quad (M, \phi) \in \text{Mp}_2(\mathbb{Z}),$$

and is holomorphic at the cusp. We write $M_l(\rho_A)$ for the space of such modular forms. The group $O(A)$ acts on $M_l(\rho_A)$ naturally through its action on $\mathbb{C}A$. Our purpose is to compute the dimension of the invariant part $M_l(\rho_A)^{O(A)}$. This is related to constructing modular forms for the full orthogonal group of an even lattice by means of lifting [2]. Let $(\mathbb{C}A)^{O(A)}$ be the $O(A)$ -invariant subspace of $\mathbb{C}A$. As its basis we can take

$$v_{[x]} = \sum_{y \in O(A)x} \mathbf{e}_y, \quad [x] \in O(A) \backslash A.$$

Since the ρ_A -action commutes with the $O(A)$ -action, it preserves $(\mathbb{C}A)^{O(A)}$. We write ρ_A^{inv} for the restriction of ρ_A on $(\mathbb{C}A)^{O(A)}$. Then

$$M_l(\rho_A)^{O(A)} = M_l(\rho_A^{inv}),$$

so the problem is to compute the dimension of the space of ρ_A^{inv} -valued modular forms. We write

$$d_A^{inv} = \dim(\mathbb{C}A)^{O(A)} = |O(A) \backslash A|.$$

If $\lambda \in \mathbb{Q}/\mathbb{Z}$, we denote by $\alpha(\lambda)$ its representative in $[0, 1)$. We set

$$\alpha(A) = \sum_{[x] \in O(A) \backslash A} \alpha(q(x)).$$

Proposition 6.1. *Let $l \equiv \sigma(A)/2 \pmod{2\mathbb{Z}}$ with $l \geq 2$. Then*

$$\begin{aligned} \dim(M_l(\rho_A^{inv})) &= \frac{d_A^{inv}(l+5)}{12} - \alpha(A) + (-1)^{(2l-\sigma(A))/4} \frac{G(A, O(A))}{4\sqrt{|A|}} \\ &\quad + \frac{2}{3\sqrt{3}\sqrt{|A|}} \operatorname{Re}\{\zeta_{24}^{Al+2-3\sigma(A)} \overline{G'(A, O(A))}\}. \end{aligned}$$

When $l \not\equiv \sigma(A)/2 \pmod{2\mathbb{Z}}$, we have $M_l(\rho_A^{inv}) = \{0\}$.

Proof. Since $\rho_A(Z)$ maps \mathbf{e}_x to $\sqrt{-1}^{-\sigma(A)}\mathbf{e}_{-x}$, we have

$$\rho_A(Z)(\mathbf{e}_x + \mathbf{e}_{-x}) = \sqrt{-1}^{-\sigma(A)}(\mathbf{e}_x + \mathbf{e}_{-x}).$$

The invariance under Z means $\sqrt{-1}^{2l-\sigma(A)} = 1$, so we must have $2l - \sigma(A) \in 4\mathbb{Z}$. In general, for a representation ρ of $\operatorname{Mp}_2(\mathbb{Z})$ such that $\rho(Z)$ acts by the scalar multiplication by $\sqrt{-1}^{2l}$, a general dimension formula for ρ -valued modular forms of weight l is given by Skoruppa (see, e.g., [3] p. 129). In the present case, it takes the form

$$\begin{aligned} \dim(M_l(\rho_A^{inv})) &= \frac{d_A^{inv}(l+5)}{12} - \alpha(A) + \frac{1}{4} \operatorname{Re}(\zeta_8^{2l} \operatorname{tr}(\rho_A^{inv}(S))) \\ &\quad + \frac{2}{3\sqrt{3}} \operatorname{Re}(\zeta_{12}^{2l+1} \operatorname{tr}(\rho_A^{inv}(ST))). \end{aligned}$$

We shall show that

$$\begin{aligned}\mathrm{tr}(\rho_A^{\mathrm{inv}}(S)) &= \zeta_8^{-\sigma(A)} \sqrt{|A|}^{-1} \cdot G(A, \mathcal{O}(A)), \\ \mathrm{tr}(\rho_A^{\mathrm{inv}}(ST)) &= \zeta_8^{-\sigma(A)} \sqrt{|A|}^{-1} \cdot \overline{G'(A, \mathcal{O}(A))}.\end{aligned}$$

We use the natural basis $v_{[x]}$ of $(\mathbb{C}A)^{\mathcal{O}(A)}$ to compute the traces. Then

$$\begin{aligned}\zeta_8^{\sigma(A)} \sqrt{|A|} \cdot \rho_A(S)(v_{[x]}) &= \sum_{x' \in \mathcal{O}(A)x} \sum_{y \in A} e(-(x', y)) \mathbf{e}_y \\ &= \sum_{[y] \in \mathcal{O}(A) \setminus A} \sum_{y' \in \mathcal{O}(A)y} \sum_{x' \in \mathcal{O}(A)x} e(-(x', y')) \mathbf{e}_{y'} \\ &= \sum_{[y] \in \mathcal{O}(A) \setminus A} \sum_{y' \in \mathcal{O}(A)y} \langle [y'], [x] \rangle_A \mathbf{e}_{y'} \\ &= \sum_{[y] \in \mathcal{O}(A) \setminus A} \langle [y], [x] \rangle_A v_{[y]}.\end{aligned}$$

This gives the trace formula for $\rho_A^{\mathrm{inv}}(S)$. For ST we have

$$\rho_A(ST)(\mathbf{e}_x) = \zeta_8^{-\sigma(A)} \sqrt{|A|}^{-1} \cdot \sum_{y \in A} e(q(x)) e(-(x, y)) \mathbf{e}_y$$

and hence

$$\begin{aligned}\zeta_8^{\sigma(A)} \sqrt{|A|} \cdot \rho_A(ST)(v_{[x]}) &= \sum_{[y] \in \mathcal{O}(A) \setminus A} \sum_{y' \in \mathcal{O}(A)y} \sum_{x' \in \mathcal{O}(A)x} e(q(x)) e(-(x', y')) \mathbf{e}_{y'} \\ &= \sum_{[y] \in \mathcal{O}(A) \setminus A} \sum_{y' \in \mathcal{O}(A)y} e(q(x)) \langle [y'], [x] \rangle_A \mathbf{e}_{y'} \\ &= \sum_{[y] \in \mathcal{O}(A) \setminus A} e(q(x)) \langle [y], [x] \rangle_A v_{[y]}.\end{aligned}$$

This gives the trace formula for $\rho_A^{\mathrm{inv}}(ST)$. □

REFERENCES

- [1] Berndt, B. C.; Evans, R. J.; Williams, K. S. *Gauss and Jacobi sums*. John Wiley & Sons, 1998.
- [2] Borchers, R. *Automorphic forms with singularities on Grassmannians*. Invent. Math. **132** (1998), no. 3, 491–562.
- [3] Eholzer, W.; Skoruppa, N.-P. *Modular invariance and uniqueness of conformal characters*. Comm. Math. Phys. **174** (1995), no. 1, 117–136.
- [4] Gerstein, L. J. *Basic quadratic forms*. Grad. Stud. Math., **90**. American Mathematical Society, 2008.
- [5] Morrison, D. R.; Saitō, M.-H. *Cremona transformations and degrees of period maps for K3 surfaces with ordinary double points*. Algebraic geometry, Sendai, 1985, 477–513, Adv. Stud. Pure Math., **10**, North-Holland, 1987.
- [6] Wall, C. T. C. *Quadratic forms on finite groups, and related topics*. Topology **2** (1963) 281–298.

DEPARTMENT OF MATHEMATICS, TOKYO INSTITUTE OF TECHNOLOGY, TOKYO 152-8551, JAPAN
E-mail address: `ma@math.titech.ac.jp`